Math 116: Worksheet 4

Owen Jones

2/8/2024

1. I used pow$(18491332, 2, 20979031)$ and checked it was equal to 43^2.

2. (a) From Euclid's lemma, if $p \mid (x-3)(x+3)$ then $p \mid (x-3)$ or $p \mid (x+3)$. Thus, $x \equiv \pm 3 \pmod{p}$.

   (b) $x = 459$

3. Suppose $x^2 \equiv y^2 \pmod{n}$. It follows $x^2 \equiv y^2 \pmod{a}$ and $x^2 \equiv y^2 \pmod{b}$. Thus, $x \equiv \pm y \pmod{a}$ and $x \equiv \pm y \pmod{b}$. Choose x s.t $x \equiv y \pmod{a}$ and $x \equiv -y \pmod{b}$. Thus, $x \not\equiv \pm y \pmod{n}$ because we have either $x \equiv y \pmod{a}$ or $x \equiv -y \pmod{b}$.

4. It passes for all except 7. Definitely composite.

5. Fails to pass Miller Rabin $a = 3$. 5197 is a factor.

In [81]:

```
import numpy as np
import math
import math116
from collections import Counter
```

In [6]:

```
math116.inverse(11,19)
```

Out[6]:

```
7
```

In [8]:

```
math116.euclidean(11,19)
```

Out[8]:

```
(1, 7, -4)
```

In [12]:

```
(3*7*11+3*4*19)
```

Out[12]:

```
459
```

In [14]:

```
n=9006401
```

In [21]:

```
(n-1)/64
```

Out[21]:

```
140725.0
```

In [22]:

```
(2**140725)%9006401
```

Out[22]:

```
1680600
```

In [23]:

```
1680600**2%9006401
```

Out[23]:

```
9006400
```

In [24]:

```
9006400**2%9006401
```

Out[24]:

```
1
```

In [26]:

```
n/(1680600+1)
```

Out[26]:

```
5.359035844915003
```

In [102…

```
def Miller_Rabin(n,a):
    m=n-1
    k=0
    while m%2==0:
        m//=2
        k+=1
    b_0=a**m%n
    if b_0==1 or b_0==n-1:
        return True
    else:
        for _ in range(k-1):
            b_1=b_0**2%n
            if b_1==n-1:
                return True
            elif b_1==1:
                return math.gcd(n,b_0-1)
            else:
                b_0=b_1
        if b_0%n!=n-1:
            return math.gcd(n,b_0-1)
```

In [111…

```
Miller_Rabin(9006401,3)
```

Out[111…

```
5197
```

In [112…

```
def Fermat(n,a):
    if a**(n-1)%n==1:
        return True
    else:
        return False
```

In [116…

```
Fermat(9006401,7)
```

Out[116…

```
False
```

In [ ]: